Rooting Out Malicious Code in Enterprise Applications

Application exposures of all types are beginning to get more scrutiny these days, but one category in particular has the full attention of IT executives.   For years malicious code - hidden in applications, awaiting activation to bring applications to their knees – has been a persistent, priority one problem for which there's been no credible, cost-effective solution. Primeon's DeepSource application audits now allow organizations to solve this problem once and for all.

What is Malicious Code?

It's hidden and extremely dangerous. "Malicious code" is a term used to designate insider modification of an organization's application(s) that introduces additional operational risk.   The insider may be an employee or a contractor working for the organization – but in either case, malicious code results when unauthorized functionality imperils the integrity of the application or its data resources is added to an application.

It comes in many forms (e.g., viruses, worms, Trojan Horses, attack scripts, Java attack applets and dangerous ActiveX controls) and has the potential to exact many levels of damage, from nuisance to catastrophic. With the trend towards offshore contracting for application development and maintenance now firmly established, government regulators are directing companies to thoroughly examine their applications for "surprises" added by the outsourcing firm (FFIEC December 2002 IT Security Handbook).

Costs when malicious code is leveraged are typically in the millions of dollars per incident. An engineering firm saw its stock price halved when it was made public that a disgruntled employee set off a logic bomb that deleted critical data.   Several large financial services companies have watched in horror as critical customer data was lost or exposed, or as fraudulent transactions were executed.

How it Works

Malicious code can take advantage of potential application weaknesses on one or several levels, including business logic, development/administration processes, architecture and/or configuration:

- Business Logic – This means using the basic functionality of the application (i.e., specified and intended functionality) to do damage. Examples would be logic bombs that delete key files, initiating illegal financial transactions, etc.

- Application Development/Administration Processes – Developers and administrators often seek the convenience of remote management capabilities. While not necessarily introduced to the application out of an initial intent to do harm, "back doors" (also called maintenance hooks) can be used by disgruntled insiders or skilled hackers to do a great deal of damage.

- Architecture – Convenience and ease of use requirements are at the root of many malicious coding incidents. Single sign-on and other access control functions designed to simply the user experience, make the malicious hacker's job easier (and multiply his impact). For example, architectural designs that allow attackers to upgrade their passwords and achieve root-level permissions are obviously at odds with the company's best interests … yet they are everywhere.

- Configuration – Similar to architecture issues above, decisions about configuring infrastructure components can play a significant role enabling malicious code situations and amplifying their impact.

Current Defenses vs. DeepSource

While ethical hackers and scanning tools have effectiveness scanning for known malicious code like viruses and worms, these approaches are equally inept when it comes to identifying one of an enterprise's biggest fears - unknown malicious code. Quite simply, without a reference or a link to the code, ethical hackers "don't know what they don't know."

By providing the complete view of an application, Primeon's DeepSource audits dramatically reduce application risk by identifying all exposures, regardless of the intent that caused them. Primeon achieves nearly exhaustive coverage by going straight to the source (code) and bringing its extensive application audit experience (and proprietary application risk knowledge base) to bear.

Benefits

While the annual loss expectancy (ALE) per application savings are substantial, to better understand some of the most important benefits, consider DeepSource from the would-be attacker's point of view. First of all, DeepSource is the first practical solution that gives organizations a credible weapon against malicious code and those who create it. As such, organizations can use DeepSource to track down, identify, and ultimately prosecute malicious coders. A secondary effect is that when malicious coders witness the efficacy of DeepSource first hand, they are compelled to remove the code they've placed for fear of being prosecuted themselves.

A Practical Solution to Malicious Code Detection and Removal

Primeon has been providing enterprise-wide source code analysis and remediation to large banks and brokerages since 1995, spanning every programming language and application architecture – over 500 millions lines of source content in all. Captured in its proprietary application security knowledge base, the collected intelligence from all previous source code audits gives Primeon an overwhelming advantage over other companies attempting to solve this problem.

Primeon's source-code centric application security offering – DeepSource – consistently provides extraordinary results with its ability to identify virtually all security exposures in critical applications and their infrastructure components. This is an order-of-magnitude improvement over the capabilities of application security tools and services and comprises the foundation of the industry's only complete solution to the pervasive application risk challenge.